Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ashley Madison Pact Spotlights Cross-Border Enforcement

By **Allison Grande**

Law360, New York (December 15, 2016, 4:17 PM EST) -- A $1.6 million settlement the Federal Trade Commission and state attorneys general recently reached with infidelity site Ashley Madison over its massive 2015 data breach highlights increased collaboration between privacy regulators in the U.S. and abroad, as well as the increasingly costly nonmonetary consequences of failing to make data security a top priority.

The FTC with attorneys general from New York, Vermont, Maryland, 10 other states and Washington, D.C., revealed the settlement with Ashley Madison parent company Ruby Corp. and two other related entities Wednesday, which stems from a July 2015 intrusion that exposed account and profile information belonging to roughly 36 million users.

The regulators' efforts to hold the Ashley Madison operator accountable for the site's lax data security and deceptive use of fake female profiles to lure subscribers was bolstered by help from privacy regulators in Canada and Australia, which issued a scathing joint report in August bashing Ashley Madison for its lax security and worked with the FTC to share information that helped their investigation into the infidelity site.

"What's noteworthy about this settlement is the cross-border coordination by regulators internationally and in the U.S. at both the federal and state level," said Craig A. Newman, a partner at Patterson Belknap Webb & Tyler LLP and chair of its privacy and data security practice group. "The footprint for many companies that operate with an online presence transcend jurisdictional borders, and this is a good example of that."

As all of these regulators have focused more intensely on data security and privacy issues in recent years, it's reasonable to believe that this type of cooperation will only become more common, making it vital for companies to pay attention to how the regulators approached this foray into cross-border cooperation, attorneys say.

"What we're seeing with this settlement is the FTC moving in a direction that's more closely aligned with the requirements for data security on an international level," Nelson Mullins Riley & Scarborough LLP attorney Bess Hinson said.

For example, while the FTC has not been shy about going after companies such as LabMD and Wyndham in the wake of data breaches, those enforcement actions have typically focused on the compromise of traditional data like payment card data and personal information such as names and Social Security

numbers. But the Ashley Madison case offers a different twist, in that it involves personal data such as photographs and sexual inclinations.

"Here, we're seeing the treatment of personal information in terms of how the FTC defines that term evolve a little bit," Hinson said. "Information like consumers' sexual preferences, photographs and online contact information strike me as an evolution of personal information towards the [European Union] definition of personal data."

The potential influence of working with international privacy regulators also peeks through in the terms of the consent decree Ashley Madison reached with the FTC.

Under that agreement, the website operator agreed to the fairly standard provision that it would implement a comprehensive data security program and have its practices assessed by an independent third party every two years. But the FTC settlement requires Ashley Madison to go a step further by ensuring that the auditor not is only qualified and objective but also holds a qualification such as certified information security professional or certified information systems auditor.

The pact also mandates that Ashley Madison designate an employee to coordinate and be responsible for the new information security program, and that the company identify and assess internal and external security risks.

"Those provisions sound to me more like what we're seeing in the general data protection regulation that will be coming up in Europe in 2018," Hinson said.

The long list of actions required by the new data security program and accompanying audits is also likely to impose a significant cost on the Ashley Madison operator that will offset some of the scrutiny over the company's relatively low monetary penalty. While the consent decrees lodged by the FTC and various state attorneys general taken together impose a total judgment of $17.5 million on the website operator, the company will only have to immediately fork over $1.6 million, with the rest suspended due to its inability to pay, the regulator said Wednesday.

"Part of the story here is that while the settlement amount might initially appear small to U.S. companies, the cost of carrying out assessments and complying with various orders from the states and from other governments is a big burden," Hinson said.

The terms of the settlement, as with previous pacts announced by the FTC and state regulators, also provide companies with a road map to building a robust data security program, which businesses would be wise to heed in order to avoid what is likely to be growing scrutiny not just in the U.S. but also abroad.

"The action is a reminder to all kinds of companies that have personal data — even some that may not be thinking about compliance as a first tier issue — about the importance of protecting this data," Wiley Rein LLP privacy practice chair Kirk Nahra said.

Specifically, the FTC's settlement serves as a reminder that when a company promises to protect sensitive information, "they must at least prepare a written information security policy, implement reasonable access controls, provide security training to employees, be aware of the security measures their service providers are using, and monitor the effectiveness of their system security," said Shook Hardy & Bacon LLP data security and privacy group co-chair Al Saikali.

"This is good advice for all companies," Saikali said.

Heeding the advice could also pay significant dividends down the road, attorneys noted. Hinson pointed to a Georgia federal court's recent decision to dismiss a putative shareholder derivative suit brought against Home Depot in the wake of its own high-profile data breach.

In reaching his conclusion that the shareholders had failed to demonstrate that board members "consciously failed to act" to prevent the breach, U.S. District Judge Thomas W. Thrash Jr. cited various steps taken by the executives, such as implementing a data security program and assessing risks, before the breach.

"So while there may not be a federal data security law and other states may not have strict requirements such as Massachusetts when it comes to data security, we have seen that, subsequent to a data breach event, if a company had taken actions to assess the risk, that puts it in a much better position than doing nothing," Hinson said.

Ashley Madison is also fighting multidistrict litigation brought by users over the hack, and both the existence of the regulatory settlements and questions over the strength of the preemptive measures the company took to safeguard user data are likely to loom large.

"While settlements aren't normally admissible in court, it's a fact that's out there, and with something as high-profile as this it may factor in," said Brenda Sharton, a Goodwin Procter LLP litigation partner and chair of its privacy and cybersecurity practice.

In its settlement Wednesday, the regulators also dinged the company for using "fembots" to impersonate real women and trick users into signing up for paid memberships and for falsely claiming that its site was 100 percent secure, a move that should drive home an important and established lesson of the importance of being honest with consumers.

"Saying a system is 100 percent secure is 100 percent a bad idea because no system is that way," Davis & Gilbert LLP partner Gary Kibel said.

The settlement is also notable in that the FTC seized upon its authority under the Section 5 of the FTC Act to police both deceptive and unfair practices, the latter of which is under attack in an appeal that LabMD is pressing before the Eleventh Circuit that found the lab's data security practices to be unfair.

"In support of its unfairness claim, the FTC complaint specifically addresses the impact of the breach on consumers, whose sexual preferences and other highly sensitive information became widely available on the web," said Janis Kestenbaum, a partner at Perkins Coie LLP and former senior legal adviser to current FTC Chairwoman Edith Ramirez. "At the same time, the FTC does not go so far as to allege that harm was 'probable,' which is notable since the Eleventh Circuit, in recently staying the FTC's LabMD decision, has called into question whether the FTC's unfairness authority extends to conduct that makes injury more likely but that does not go so far as to make it 'probable.'"

While uncertainty lingers about the direction the FTC will take under the incoming Trump administration and how aggressively it will push its unfairness authority in data security cases going forward, attorneys say that it is more likely than not that global regulators will continue to focus heavily on this issue, and that the FTC won't back down from the momentum it has built with its most recent enforcement action.

"Broadly speaking, this case is telling when it comes to the FTC's priorities," said Heather Egan Sussman, co-chair of Ropes & Gray LLP's privacy and data security practice. "It shows that while the FTC's enforcement has recently been focused on alleged product insecurities, the agency is still being aggressive and poses a risk to businesses of all types when their own systems are breached."

--Editing by Brian Baresch and Catherine Sum.
